Brooklyn Law Review

Volume 81 | Issue 1 Article 9

2015

If You Give a Mouse a Cookie, It's Going to Ask for Your Personally Identifiable Information

Julia N. Mehlman

If You Give a Mouse a Cookie, It's Going to Ask for Your Personally Identifiable Information

A LOOK AT THE DATA-COLLECTION INDUSTRY AND A PROPOSAL FOR RECOGNIZING THE VALUE OF CONSUMER INFORMATION

INTRODUCTION

Picture yourself in the grocery store walking up and down the aisles, browsing the shelves in search of the ingredients for that complicated recipe you found on the Food Network website. Now picture someone following you, standing right behind you every step of the way, taking notes on everything you do. You looked at four brands of sugar but decided that for your key lime pie, the generic brand would be best (or is it because it is the cheapest?). You chose three limes that looked less than green, but they were the biggest ones on the shelf and the sale price was 75 cents per lime. After walking down the candy aisle, you turned right for paper goods instead of left for frozen foods. Oh, and this is interesting, you put a package of diapers in your shopping cart. You must have a baby at home.

If you would find this uncomfortable, you are not alone. The tailgater is in clear violation of the social norm commonly referred to as "personal space,"[1] which extends at least one and a half feet from the center of a person's body.[2] Although invasions of personal space are sometimes an unavoidable fact of everyday life (e.g., the subway at rush hour), certain impersonal situations, such as grocery shopping, do not warrant an intrusion into the invisible bubble that protects individuals from unwanted contact and interaction. If this idea theoretically protects a grocery store patron from being followed too closely, what changes when this activity occurs in the virtual space?

---

[1] *See generally* EDWARD T. HALL, THE HIDDEN DIMENSION (1966) (introducing the concept of personal space and "proxemics").

[2] *Id.* at 112-25.

The amount of information that exists in virtual space is almost unfathomable,[3] not only to a human being who processes information in ways other than just 1s and 0s, but even to some advanced technologies that *only* understand 1s and 0s. This incredible amount of data, unmanageable by traditional electronic data storage systems, is referred to as "Big Data."[4] This data comes from all over the Internet and contains just about anything and everything imaginable, including consumer information, user web activity, and other personal information about individual Internet users. This information is not just sitting on a computer somewhere taking up an exorbitant amount of space. On the contrary, this often personal information is being collected, deciphered, and sold for enormous sums of money without the knowledge of the users from whom the information originates[5] and without remuneration to these unknowing subjects. Data brokers provide this collected information to their clients and have largely managed to remain hidden from public scrutiny.[6] As knowledge of this practice increases, however, data brokers have experienced more pressure to shed their veils of secrecy and become officially present as the major market players that they are. Because the data-collection industry is largely unregulated, there has been much discussion and debate regarding future regulation and how best to balance the interests of the market with the interest of consumers.[7]

This note examines the lack of regulation and transparency surrounding the data-collection industry, as well as recent proposals aimed at alleviating concerns about these regulatory deficits. It suggests that, to ease tension with consumers, data brokers should share a portion of the profits that they gain from

---

[3] Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, HARV. BUS. REV. (Oct. 2012), http://hbr.org/2012/10/big-data-the-management-revolution/ar [http://perma.cc/2ZR4-948Q] (noting that as of 2012, 2.5 exabytes of data were being created daily). One exabyte equals one quintillion bytes—that's 10^{18} bytes. To put this in perspective, no single computer storage system in the world can hold even close to an exabyte of data. The measurement of an exabyte can only be used in the context of measuring multiple storage systems. *Exabyte Definition*, TECHTERMS, http://www.techterms.com/definition/exabyte [http://perma.cc/RXX6-78NP] (last updated Dec. 7, 2012).

[4] Edd Dumbill, *What Is Big Data?*, O'REILLY RADAR (Jan. 11, 2012), http://radar.oreilly.com/2012/01/what-is-big-data.html [http://perma.cc/JB4D-YLV4] (defining "big data" in terms of the technological capacity to decipher and store).

[5] S. COMM. ON COMMERCE, SCI., AND TRANSP., A REVIEW OF THE DATA BROKERS INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 5 (Dec. 18, 2013) http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577 [http://perma.cc/C99L-M24S] [hereinafter SENATE COMMERCE COMMITTEE].

[6] *Id.*

[7] *See infra* Part IV.

distributing consumer information to third parties. This type of compensation is essential to strengthening the fabric that connects the data-collection industry to consumers and fundamental notions of personal integrity, privacy, and self-worth.

Part I of this note introduces the data-collection industry, including the types and sources of collected information. Additionally, this Part details the prominent role that data collection plays in the U.S. market economy and how it has quickly become a multibillion dollar business.

Part II recognizes the benefits associated with the presence of data brokers, explains the advantages conferred upon client companies who enlist the services of data brokers, and acknowledges the benefits to consumers.

Part III discusses the concerns associated with the emergence of the data-collection industry, including the lack of transparency between data brokers and Internet users, privacy issues, and the pervasiveness of the Internet in a modern world that is largely dependent on technology. This Part discusses how these concerns might be addressed while still accounting for the interests of all relevant parties.

Part IV explores the current state of both federal and state laws regulating data collection, as well as recent proposals to fill the regulatory void. In addition, this Part examines applicable privacy laws as they pertain to electronic storage systems. It also details the Federal Trade Commission's past and current roles in attempting to regulate the data-collection industry and its possible rule-making position in the future.

In conclusion, Part V introduces a proposal, inspired by the theory of unjust enrichment, to ease the tension between data brokers and consumers: data brokers should compensate consumers for their collected information as a way of recognizing and legitimizing the information's value. This Part seeks to identify why courts have held this idea to be inappropriate, and it respectfully disagrees, offering an alternative solution involving consumer compensation. Finally, this Part discusses why it is important that the data-collection industry recognize value in an individual's dossier of personal information and explains how the proposed solution will strike a balance between data brokers' and consumers' interests.

I. DATA BROKER? I HARDLY KNOW HER

In order to accurately assess the privacy implications of widespread data collection, it is first important to understand who data brokers are, what they do, and how they collect information.

This Part defines "data brokers" and provides a basic understanding of how they collect information. It then identifies the sources from which data brokers collect such information. The final section discusses the role that data brokers play in the American economy.

A. Data Brokers and How They Collect Information

Although there is no statutory definition of the term "data brokers" (also referred to as information brokers, data aggregators, and data collectors), the Federal Trade Commission (FTC) defines data brokers as "companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes."[8] While the practice of mass data collection is not new in the United States,[9] recent technological developments have transformed the data-collection industry by increasing the ease of access to consumer information.[10] Information that used to take a trip to a library or a courthouse to find is now easily obtained by a click of a button.[11] Data aggregators can find this information with such ease because all Internet users leave behind a digital footprint.[12]

An Internet user's digital footprint is made up of every single thing the user does on the web.[13] Digital footprints

---

[8] SENATE COMMERCE COMMITTEE, *supra* note 5, at 1 (quoting FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 68 (Mar. 2012)).

[9] In 1790, the First Congress conducted the first U.S. census. *1790*, U.S. CENSUS BUREAU, https://www.census.gov/history/www/through_the_decades/overview/1790.html [http://perma.cc/4XYD-FX3E] (last visited Dec. 11, 2015). Every 10 years since then, the United States Census Bureau has conducted a constitutionally mandated Population and Housing Census. *What We Do*, U.S. CENSUS BUREAU, https://www.census.gov/about/what.html [http://perma.cc/GVG5-C3T4] (last visited Dec. 11, 2015). In 1880, the Census Bureau experienced a premature instance of what is now commonly referred to as "information overload." The data compiled for the 1880 census took an unprecedented eight years to tabulate. *Tabulating and Processing*, U.S. CENSUS BUREAU, https://www.census.gov/history/www/innovations/technology/tabulation_and_processing.html [http://perma.cc/M8PL-7L6S] (last visited Dec. 11, 2015).

[10] For an incredible real-time website demonstrating just how much technology has transformed the manner and ease with which we are able to receive information, see *United States Internet Users*, INTERNET LIVE STATS, http://www.internetlivestats.com/watch/internet-users/region/ [http://perma.cc/S9TY-5NAE] (last visited Dec. 11, 2015).

[11] SENATE COMMERCE COMMITTEE, *supra* note 5, at 1-2.

[12] *What Is a Digital Footprint?*, INTERNET SOC'Y (Jan. 28, 2014), http://www.internetsociety.org/sites/default/files/flash/What_is_a_Digital_Footprint/presentation_content/external_files/What_is_a_Digital_Footprint.pdf [http://perma.cc/ZH6V-HKMC].

[13] PEW INTERNET & AM. LIFE PROJECT, DIGITAL FOOTPRINTS: ONLINE IDENTITY MANAGEMENT AND SEARCH IN THE AGE OF TRANSPARENCY 2 (2007), http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf. [http://perma.cc/GN8S-7ZG5] [hereinafter PEW INTERNET]. For an interesting discussion of

contain public activity, such as posts and comments made on social media websites, as well as some not so public activity, such as an archived list of all the terms entered into the Google search bar.[14] Digital footprints are like footprints in the sand. When people walk along the shore, they leave footprints. These footprints let others know that someone has been there before and might possibly reveal information about that person's destination. However, "[u]nlike footprints left in the sand at the beach, . . . online data trails often stick around long after the tide has gone out."[15] The everlasting quality of the digital footprint as an enduring source of collectable information makes it appealing to data brokers.

In addition to the digital footprints that Internet users leave behind, cookies are one of the most useful tools in the data-collection industry's repertoire. While these cookies are not the delicious type that probably come to mind at first blush, they are equally enticing to data brokers and any entity on the Internet seeking to collect user information. Cookies are small text files "used in internet advertising to store website preferences, retain the contents of shopping carts between visits, and keep browsers logged into social networking services as individuals surf the internet."[16] When a user visits a website for the first time, the website places a cookie on the user's computer.[17] The text file contains a unique string of letters and numbers, called a name-value pair, which is used to identify the user when she visits the webpage in the future; this is called a "first-party cookie."[18] Similarly, a party other than the actual website the user has visited may place a "third-party cookie" on the user's computer.[19] To illustrate, many websites reserve space for third parties to advertise on their web pages for a fee. When a user visits a site like this, the user's computer will receive a first-party cookie from

---

the concept of digital footprints and the "shift from the ephemeral to the eternal," see John Battelle, *From the Ephemeral to the Eternal*, JOHN BATTELLE'S SEARCHBLOG (May 6, 2004), http://battellemedia.com/archives/2004/05/from_the_ephemeral_to_the_eternal.php [http://perma.cc/CBB7-JZ3L].

[14] PEW INTERNET, *supra* note 13, at 2-3 ("The five most popular search engines routinely archive a user's search terms, their computer address, and the unique identifier for their Web browser for 13-18 months." (citing CTR. FOR DEMOCRACY & TECH., SEARCH PRIVACY PRACTICES: A WORK IN PROGRESS (Aug. 2007))).

[15] *Id.* at i.

[16] *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d. 434, 439-40 (D. Del. 2013).

[17] Many websites actually place multiple cookies on a user's computer. But for the sake of simplicity and ease of explanation, speaking in terms of one cookie is sufficient.

[18] *In re Google Inc.*, 988 F. Supp. 2d. at 440.

[19] *Id.*

the host site and a third-party cookie from the entity whose advertisement appears on the first-party host site.[20] Data brokers collect the information that the third-party cookies gather and compile this information for their clients in order to "promote products to consumers more effectively through a [highly] customized user experience."[21] This is why all of the websites you visit somehow just *know* that you are a skier trying to book a trip to Aspen this coming winter and that you happen to have recently browsed Gap's online store for a new coat. Although information that cookies gather from a user's computer is often pseudonymized, meaning this information cannot independently identify an individual person, there are still very valid and legitimate privacy concerns associated with the cookie collection method.[22]

B. The Categories of Collection

The breadth of information that data brokers collect is enormous. In December 2012, the FTC conducted a study to explore the habits of nine major data brokers.[23] The study reported that the companies collect from sources "[that] fall into three [major] categories: (1) government sources; (2) other publicly available sources; and (3) commercial sources."[24] All three categories contain data points that can be associated with a specific individual's online and offline presence.

---

[20] *Id.*

[21] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 26 (2014), http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [http://perma.cc/KQ6S-CCCS] [hereinafter DATA BROKERS].

[22] See *infra* Part III, discussing privacy concerns associated with data collection.

[23] DATA BROKERS, *supra* note 21, at 7. The FTC issued Orders to File Special Reports to each of the "nine data brokers pursuant to Section 6(b) of the Federal Trade Commission Act, 15 U.S.C. § 46(b)." *Id.* at 3. This section of the Act states in relevant part that the FTC has the power

> to require, by general or special orders, persons, partnerships, and corporations, engaged in or whose business affects commerce, . . . to file with the Commission in such form as the Commission may prescribe annual or special, or both annual and special, reports or answers in writing to specific questions, furnishing to the Commission such information as it may require as to the organization, business, conduct, practices, management, and relation to other corporations, partnerships, and individuals of the respective persons, partnerships, and corporations filing such reports or answers in writing.

15 U.S.C. § 46(b) (2006). The nine data brokers that received the Orders are as follows: Acxiom, Corelogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf, and Recorded Future. DATA BROKERS, *supra* note 21, at 8-9.

[24] DATA BROKERS, *supra* note 21, at 11.

Information from government sources comes from federal, state, and local governments.[25] This category includes information from the U.S. census, the social security numbers and dates of death contained in the Social Security Administration's Death Master File, and any professional licenses and motor vehicle records distributed by states.[26] Category two, consisting of other publicly available sources, contains the bulk of information obtained.[27] This category includes information posted on social media websites, blogs, and other publicly accessible Internet forums.[28] For example, data brokers can take advantage of online profiles when users fail to "restrict access to their information."[29] When these profiles are set to "public," it allows data brokers to freely collect information associated with the account. Given the explosion of social media culture in the past decade, one can imagine the immeasurable amount of collectable data available to data brokers from the buffet of interactive platforms in existence.

Although it covers arguably the widest range and variety of information collected, many consumers may fail to realize that the final category even exists. This category consists of information gathered from commercial sources, such as "retailers and catalog companies," magazine and online subscriptions lists, purchase lists from financial service companies, and information that data brokers share with one another.[30] For example, companies and data brokers use store loyalty cards to collect information about the specific products customers purchase and how often they purchase them.[31] When a customer signs up for a rewards program, he or she gives out some standard information. At a minimum, this includes first and last name, possibly an email address, and maybe a home address and phone number. Even if the consumer provides only his or her name, that is enough for the store's data broker to link the consumer's real world and virtual presence.[32]

---

[25] *Id.*

[26] *Id.* at 11-12.

[27] *Id.*at 13.

[28] *Id.*

[29] *Id.*

[30] *Id.* at 13-14.

[31] "Datalogix, . . . which collects information from store loyalty cards, says it has information on more than $1 trillion in consumer spending 'across 1400+ leading brands.'" Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014, 1:59 PM), http://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you [http://perma.cc/MV2K-EUSK]; *see* SENATE COMMERCE COMMITTEE, *supra* note 5, at 16.

[32] "Datalogix . . . has partnered with Facebook to track whether Facebook users who see ads for certain products actually end up buying them at local stores . . . ." Beckett,

Although "[m]uch of the information [collected in each of the three categories] is demographic, such as consumers' names, addresses, telephone numbers, gender, [and] age,"[33] a great deal of the information collected is of the type that an average person might consider "sensitive" and would ordinarily take more in-depth investigation to obtain.[34] For example, many data brokers collect health-related information, such as whether a particular person "uses laxatives or yeast infection products[, and the number of] OB/GYN doctor visits within the last 12 months."[35]

C. Data Collection's Role in the U.S. Economy

In addition to its clear (although often under-the-radar) presence in daily life, the data-collection industry is quickly becoming a major player in the U.S. economy.[36] In 2012, Professor

---

supra note 31, at 3. The practice of researching products online before purchasing the same product in the brick-and-mortar store is referred to as "webrooming." Mike Cassidy, *Consumers are Harnessing Tech to Return to Stores—Good News or Bad News First?*, WIRED.COM (Sept. 12, 2014, 2:24 PM), http://www.wired.com/2014/09/webrooming/ [http://perma.cc/7FL8-6G6V]. A Nielsen survey shows that "[w]hen shopping for non-consumable goods where consumers typically have something in mind, there is mostly a one-to-one correlation between online searching and shopping." *E-commerce: Evolution or Revolution in the Fast-Moving Consumer Goods World?*, NIELSEN (Aug. 26, 2014), http://www.nielsen.com/us/en/insights/reports/2014/e-commerce-evolution-or-revolution-in-the-fast-moving-consumer-goods-world.html [http://perma.cc/T5RA-AKUX].

[33] SENATE COMMERCE COMMITTEE, *supra* note 5, at 13.

[34] DATA BROKERS *supra* note 21, at 13-14 (noting that information concerning health-related purchases is often collected); *see also* SENATE COMMERCE COMMITTEE, *supra* note 5, at 14, n.62-64 (noting that at least three major companies collect information regarding the types of medical conditions that ail certain Internet users).

[35] SENATE COMMERCE COMMITTEE, *supra* note 5, at 14. Furthermore, companies may utilize data broker services to market to individuals based on the health-related information obtained. In fact, WebMD's Privacy Policy states the following:

> Third parties under contract with WebMD may use Cookies or Web Beacons to collect Non-Personal Information about your usage of the WebMD Web Sites, *including which health topics you have viewed*. These third party advertising service providers may use this information to help WebMD deliver advertising on the WebMD Web Sites as well as on other sites on the Internet based on your browsing activity on our sites.

WebMD Privacy Policy Summary, WEBMD, http://www.webmd.com/about-webmd-policies/about-privacy-policy?ss=ftr [http://perma.cc/4YW6-VCB5] (last visited Dec. 11, 2015) (emphasis added). Based on this language, WebMD may use data brokers to market to individuals based on the symptoms they input into the WebMD "symptom checker" or simply health conditions in which the user is interested.

[36] JOHN DEIGHTON & PETER A. JOHNSON, THE VALUE OF DATA: CONSEQUENCES FOR INSIGHT, INNOVATION & EFFICIENCY IN THE U.S. ECONOMY (2013); DATA BROKERS, *supra* note 21, at 23 (showing that one single year of revenue for *only nine* data brokers added up to a total of $426,742,795). A preliminary Google search for "data collection companies usa" yielded almost 300 companies in clicking on just two of the many links Google returned on the query. GOOGLE.COM, https://www.google.com/search?q=list+

John Deighton of Harvard Business School and Professor Peter A. Johnson of Columbia University conducted and published a study revealing that "the data-driven marketing economy [DDME] represented a *minimum* of $156 billion in value-added revenues for services to the U.S. economy."[37] In addition to the substantial income the DDME generated, it also "supported approximately 676,000 jobs" in that same year.[38] These figures represent the types of market services "that could not have been performed without individual-level consumer data (ILCD)," which includes both pseudonymized information and personally identifiable information.[39]

Although data brokers charge their clients pennies for individual pieces of information, once clients seek multiple data points for thousands or hundreds of thousands of individuals, the overall cost can easily add up.[40] One data broker, TowerData (formerly RapLeaf), offers 34 different categories of collectable data points.[41] Although each category is worth no more than $0.01, if a client chooses to collect information from at least one person in every single category and TowerData matches each data field to that same individual, the client will pay TowerData less than $0.50 just for these individual-level matches.[42] For buyers, data is cheap. But the amount of money that client companies make from this data is exponentially higher than the minimal cost of purchase.[43]

---

of+data+brokers+in+usa&oq=list+of+data+brokers+in+usa&aqs=chrome..69i57.4982j0j7&sourceid=chrome&es_sm=93&ie=UTF-8#q=data+collection+companies+usa [http://perma.cc/J8RH-Z2PR] (last visited Dec. 11, 2015). Once on Google.com, the search "data collection companies" yielded links to, among others, GreenBook.org, which listed 181 results "for market research firms that offer field collection services," and Quirk's.com, which listed 140.

[37] DEIGHTON & JOHNSON, *supra* note 36, at 14 (emphasis added). The authors of the study note that

> [v]alue-added revenues equate to the net amount that producers of goods and services spend on individual-level data services to find customers for their offerings, together with associated employment. . . . [They] treat this amount as a lower bound to the value added to the U.S. economy by the DDME. . . . [They] make the standard economic assumption that firms spend on inputs until the marginal cost equals the marginal return. So the surplus value created by the spending of $156 billion is likely substantially greater than that amount . . . .

Id.

[38] *Id.*

[39] *Id.* at 5. ILCD is the type of "information signal that originates with an individual consumer, or prospective consumer." *Id.* at 11.

[40] *Email Intelligence, a TowerData Solution*, TOWERDATA, http://intelligence.towerdata.com/pricing-append [http://perma.cc/3J2F-8KDW] (last visited Dec. 11, 2015).

[41] *Id.*

[42] *Id.* This price does not include base services that TowerData charges to clients.

[43] Alexis C. Madrigal, *How Much Is Your Data Worth? Mmm, Somewhere Between Half a Cent and $1,200*, ATLANTIC (Mar. 19, 2012, 3:18 PM),

II. THE BENEFITS OF DATA COLLECTION

While much of the negative commentary about data collection focuses on privacy concerns, it is important to acknowledge the benefits that the data-collection industry provides to society as a whole. This Part explores some of the advantages that data-collection firms bestow upon their client companies and consumers, a fact that should not be forgotten when proposing solutions to ameliorate privacy concerns.

A. Benefits to Client Companies

From a business standpoint, data-collection firms offer many valuable and innovative solutions to clients. These solutions can be divided into three main categories: "marketing" products, "risk mitigation" products, and "people search" products.[44]

1. Marketing Products

Marketing products "enable . . . clients to create tailored marketing messages to consumers."[45] These products are further divided into three subgroups: "direct marketing," "online marketing," and "marketing analytics."[46] Direct marketing products allow clients to "learn more about their customers" by "help[ing] . . . fill in gaps that may exist in customer contact information."[47] The client provides the data broker with some basic information about the customer, including a name and address, and the data broker will then provide other information associated with that customer.[48] Additionally, direct marketing products help "identify consumers who share particular characteristics"[49] (for example, all persons who are female, have two children, and are licensed attorneys). "The client identifies the attributes that it would like to find in a consumer audience, and the data broker provides a list of consumers with those attributes."[50] This type of information aggregation allows clients to tailor their marketing campaigns to the consumers that frequently

---

http://www.theatlantic.com/technology/archive/2012/03/how-much-is-your-data-worth-mmm-somewhere-between-half-a-cent-and-1-200/254730/ [http://perma.cc/VR5E-J73L].

44 DATA BROKERS, *supra* note 21, at 23.

45 *Id.*

46 *Id.*

47 *Id.* at 24.

48 *Id.* at 25.

49 *Id.*

50 *Id.*

use their products and helps companies reduce marketing directed at groups that are not regular consumers.[51] In employing this tactic, "[t]he gain in marketing efficiency from avoiding spillover spending onto uninterested consumers is substantial."[52]

Online marketing allows entities to market "to consumers through the Internet, mobile devices, and cable and satellite television."[53] Through this medium, companies may display "more targeted and potentially relevant advertising to consumers."[54] This allows companies to provide a more personalized and enjoyable online experience for the user. If the consumer likes what she sees when she logs on to the site, she is more likely to come back—this means more money and/or exposure for the client company.[55] Data brokers also use online marketing to help connect a consumer's online and offline activity by targeting both existing customers who already use the company's products and potential consumers whose existing dossier suggests that they might be interested in the client's products.[56] Like online marketing products, marketing analytics products "enable a client to more accurately target consumers for an advertising campaign, refine product and campaign messages, and gain insights and information about consumer attitudes and preferences."[57] Data brokers assist clients in this way by helping to "model the expected outcomes of various marketing tactics, thus allowing the clients to better advertise their products to consumers."[58]

2. Risk Mitigation Products

Risk mitigation products allow clients to verify consumer information, "confirm[] the identity of an individual," and help protect against fraudulent activity.[59] Some clients use these products to comply with state and federal laws, such as the USA

---

[51] DEIGHTON & JOHNSON, *supra* note 36, at 43 (noting that "[t]he goal of audience targeting is to put digital advertising in front of only the small proportion of consumers who are very likely to respond to it").

[52] *Id.*

[53] DATA BROKERS, *supra* note 21, at 26.

[54] *Id.* See also *infra*, Section II.B, discussing the benefits of targeted advertising to consumers.

[55] Advertisements may be tailored to the location of the user's computer or to the user's specific interests and preferences that the data broker has gathered elsewhere on the Internet.

[56] DATA BROKERS, *supra* note 21, at 28.

[57] *Id.* at 31.

[58] *Id.*

[59] *Id.* at 32.

PATRIOT Act[60] or the Fair Credit Reporting Act.[61] To assist their clients in confirming consumers' identities, data brokers offer "quiz product[s]," which can help add extra layers of identity verification.[62] These types of products are well known and typically appear when signing up for an online service.[63] For example, if a user decides to pursue online banking, the user will be prompted to choose from a bevy of "security questions" to ensure the safety of the account.[64] This both protects the user's information and guarantees to the bank that the user is in fact who she says she is. In this same vein, risk mitigation fraud detection products allow clients to assess the information a consumer submits and corroborate the reliability of such information.[65]

3. People Search Products

People search products provide information from publicly available sources, such as government records and social media platforms.[66] As mentioned in Section I.B, data brokers use information that is easily obtainable—whether in digital or paper form—due to its public nature.[67] This includes newspaper articles, online profiles set to "public," and other documents to which the public has general access. People search products take these resources and match personal information about an individual person or company with other pieces of public information and/or information already contained in a data broker's database. These tools are beneficial to both clients and consumers who utilize them when searching for a long-lost friend on Facebook or a potential love interest on Match.com.[68]

---

[60] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 107 P.L. 56, 115 Stat. 272.

[61] DATA BROKERS, *supra* note 21, at 32.

[62] *Id.*

[63] *See id.*

[64] Examples of commonly asked security questions include: "[W]here did you go to high school? [W]hat is the name of the first street you lived on?" Rebecca J. Rosen, *Security Questions: The Biggest Joke in Online Identity Verification*, ATLANTIC (Aug. 7, 2012, 5:36 PM), http://www.theatlantic.com/technology/archive/2012/08/security-questions-the-biggest-joke-in-online-identity-verification/260835/ [http://perma.cc/Z7HX-VLLR]. For an interesting take on what happens when security questions fail to protect consumer information, see *id.*

[65] DATA BROKERS, *supra* note 21, at 33.

[66] *Id.* at 34.

[67] *See supra* Section I.B.

[68] DATA BROKERS, *supra* note 21, at 34.

B. Benefits to the Consumer

Although data brokers often gear their solutions toward the client companies, these solutions also afford Internet users and consumers benefits that may be hidden behind the inherent suspicion surrounding online data collection.[69] Targeted ads confer a standout advantage on consumers by creating an enhanced Internet browsing experience.[70] In tailoring the ads that appear on their websites using first- and third-party cookies, companies are able to offer consumers a more personalized and enjoyable experience by presenting advertisements and product suggestions that appeal to individual consumers' interests.

A company will use the data it has paid for to provide ads that are "more likely to be relevant (and therefore useful) to [the consumer]."[71] Remember the ski trip you were trying to book? The banner ads that appear on websites you visit may now show hotel prices near Aspen and Vail, as well as places offering sales on ski and snowboard equipment. This type of relevant ad placement may cause the consumer to have a favorable attitude about the first-party website hosting the helpful ad and the third-party website providing the useful and relevant information. Further, it makes the consumer's life easier by pointing her in the right direction to find the products she wants.

Online services also utilize compiled data in order to cater to their users' interests. For instance, "Netflix's video recommendation feature . . . [demonstrates] how secondary uses of data can create consumer benefits."[72] The on-demand media streaming company's "personalized video recommendation feature us[es] information that Netflix originally collected" about the user's viewing preferences to suggest related titles that are similar to what the user has previously watched.[73] Similarly,

---

[69] *See* Adam Thierer, *Relax and Learn to Love Big Data*, U.S.NEWS & WORLD REP. (Sept. 16, 2013, 12:10 PM), http://www.usnews.com/opinion/blogs/economic-intelligence/2013/09/16/big-data-collection-has-many-benefits-for-internet-users [http://perma.cc/5HYP-NKDG]; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 26, 57 (2012) [hereinafter AN ERA OF RAPID CHANGE]; Dustin D. Berger, *Balancing Consumer Privacy with Behavioral Targeting*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 3, 31-34 (2011); Meredith Kile, *Need to Know: How Mobile Data Collection Benefits the Consumer*, ALJAZEERA AM. (Mar. 13, 2014, 6:30 PM), http://america.aljazeera.com/watch/shows/techknow/blog/2014/3/13/need-to-know-howmobiledatacollectionbenefitstheconsumer.html [http://perma.cc/G9AD-B9SH].

[70] *See* Berger, *supra* note 69, at 16-17 (discussing how targeted ads work via cookies).

[71] *Id.* at 3, 31-32.

[72] AN ERA OF RAPID CHANGE, *supra* note 69, at 26.

[73] *Id.* at 57.

Amazon recommends certain products to consumers based on the products they have previously browsed or purchased.[74]

Another benefit that data collection offers to both consumers and the public at large is the potential for increased technological innovation. According to one commentator:

> Many of the information services and digital technologies that . . . [society] enjoy[s] . . . came about not necessarily because of some initial grand design, but rather through innovative thinking after-the-fact about how preexisting data sets might be used in interesting new ways. Some examples include: language translation tools, mobile traffic services, digital mapping technologies, spam and fraud detection tools, instant spell-checkers and more.[75]

The possibilities that can come from this emerging technology are limitless.[76] By purchasing information about consumer interests and preferences, companies can improve their products to meet consumer demands. Additionally, consumers can benefit from the positive impact that this innovation will have on small businesses. As data collection continues to surge in the market economy, its availability to local shops will increase. The places that the consumer already knows and loves will be able to use data services to further improve the shopping experience for their loyal patrons. Although consumers often oppose data collection, it is important to keep these benefits in mind when balancing the interests of all the parties that data brokers affect.

III. WAIT A MINUTE, THIS DOESN'T FEEL RIGHT: CONCERNS ABOUT DATA COLLECTION AND WHY WE SHOULD CARE

Although data brokers offer valuable services to their clients, there are valid concerns about a practice where the person about whom information is being collected does not know, or is only loosely aware, of the existence of such entities and services. The lack of transparency surrounding the data-brokerage industry as a whole raises general concerns about possible deception and under-the-table practices. Furthermore, the privacy issue in this context is utterly unavoidable. How far is too far, and how far are we willing to let data brokers go,

---

[74] Berger, *supra* note 69, at 32.

[75] Thierer, *supra* note 69.

[76] *See generally* Steve Hemsley, *Data Collection Gets Innovative*, MARKETING WEEK (Oct. 10, 2012), http://www.marketingweek.com/2012/10/10/data-collection-gets-innovative/ [http://perma.cc/RQK3-G9WF] (noting innovative new ways to use consumer data).

particularly in light of the Internet's pervasive presence in modern life, before society collectively says, "enough"?

A. Lack of Transparency

The crux of the transparency concern is that data brokers harvest and obtain information without the consumer's knowledge or explicit consent, and consumers are largely unaware of the type of information being collected and disseminated. "Data brokers generally are not consumer facing, therefore, most consumers have no way of knowing that data brokers may be collecting their data."[77] This lack of transparency creates an intrinsic distrust between data brokers and consumers. First of all, many people are still unaware of the existence of data brokers, and for people who are aware, they are unfamiliar with the extent of information that is collected or how it is used.[78]

"Because users are not generally aware of . . . [data brokers'] methods of collection and distribution, many feel insecure about surfing the web. This anxiety increases every time the media reports stories extolling the dangers of personal information that has been bought, sold or stolen."[79] As far as ignorance being bliss, in this scenario, such ignorance, when perpetuated by the data brokers themselves, is unfair and unacceptable to the consumers from whom they are profiting so handsomely. No one likes to have the wool pulled over their eyes; no one likes to feel like they are being deceived. And when consumers find out that the companies they have been so loyal to for years have essentially talked behind their backs and spread their information to third parties, it is in that moment that they lose trust in those companies.

As discussed in the next Part, the FTC is engaged in somewhat of a crusade to remedy this lack of transparency.[80]

---

[77] SENATE COMMERCE COMMITTEE, *supra* note 5, at 32.

[78]

> Data brokers acquire a vast array of detailed and specific information about consumers; analyze it to make inferences about consumers, some of which may be considered sensitive; and share the information with clients in a range of industries. All of this activity takes place behind the scenes, without consumers' knowledge.

DATA BROKERS, *supra* note 21, at vii.

[79] David Goldman, *I Always Feel Like Someone Is Watching Me: A Technological Solution for Online Privacy*, 28 HASTINGS COMM. & ENT. L.J. 353, 369 (2006).

[80] *See* DATA BROKERS, *supra* note 21, at 3-7; s*ee also infra* Part IV (discussing the FTC's role in proposed regulation of the data-collection industry); Press Release, Federal Trade Commission, FTC Charges Data Brokers with Helping Scammer Take

Although clearly easier said than done, one way to remedy a situation like this is to ensure that people are informed. Consumers should know that their data is collected in the first place, and they should also know what is done with that information. When consumers are properly informed, they can form more educated opinions and are better suited to advocate for themselves.

B. Privacy

When it comes to criticizing data collection, the issue of privacy is quite possibly the most popular hot-button topic—this is what everyone is talking about. When people first learn about data brokers, their instant reaction is almost always one of incredulity. They next deliver a monologue about how that has got to be in violation of *some* privacy law.[81] The privacy concern in this context is a loaded one that numerous scholars have addressed in different and nuanced ways.[82]

The heart of the privacy issue is that there is something unsettling and wrong about a stranger knowing so much about another person's life without permission to be privy to that information. The stranger can piece together a cohesive picture of an individual's life by compiling hundreds of data points that are recorded about any given person. "Individually, each of these

---

More Than $7 Million from Consumers' Accounts (Aug. 12, 2015), https://www.ftc.gov/news-events/press-releases/2015/08/ftc-charges-data-brokers-helping-scammer-take-more-7-million [http://perma.cc/AJ92-S4S3] (detailing a recent charge brought by the FTC against Sequoia One, LLC, Gen X Marketing Group, LLC, and several of the companies' owners, operators, and managers, for scamming payday loan applicants and "debiting their bank accounts and charging their credits cards without their consent").

[81] While writing this note, I spoke to many people regarding data brokers, including family, friends, peers, and professionals. Many were unaware of data brokers' existence. Some were aware of their existence but did not have a detailed picture of exactly what data brokers do. The reaction mentioned above is the one I received during almost every conversation.

[82] For a more in-depth look at privacy as it relates to data brokers, see Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91 (2009) (discussing the lack of protections offered by the existing legal privacy regime and proposing the enactment of stronger laws to meet that end); Goldman, *supra* note 79, at 357 (suggesting that the best way to alleviate Internet privacy concerns is to combine aspects of various systems to create a "hybrid solution that allows individuals and marketers to work together to determine their own value for personal information"); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 7 (2003) (arguing that "information privacy should be viewed as a societal value justifying a resolution in the public interest, much like environmental policy and other societal concerns, with less emphasis on individual self-policing and market-based mechanisms"); Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433 (2014) (comparing U.S. privacy laws to the European Union's heavily regulated privacy regime and further suggesting that the European Union's approach is more favorable for protecting personal privacy and dignity).

pieces of personal information represents a mere pixel of [someone's] life, but when pieced together, they present a rather detailed picture of [that person's] identity."[83] This mosaic effect of data compilation leaves people feeling violated and anxious about who knows what and how much. Targeted ads also rub many people the wrong way. Even if companies contend that targeted ads will enhance a consumer's online experience, this still, for lack of a better phrase, "creeps out some people who see it as an invasion of their privacy."[84]

The first time I saw a targeted ad some years ago, I did not know what I was seeing or how it worked. I was confused, impressed by the extrasensory machine that I was apparently using, and also puzzled as to why and how the sidebar of the Pandora music player was displaying my latest online shopping purchase. You have to admit the strange feeling when targeted ads show up on an unrelated webpage—a "how did you know that when I did not tell you" sort of feeling that is off-putting and odd.

When it comes to their online presence, people are not necessarily concerned about privacy because they have something to hide. Rather, when an unauthorized entity has the ability to obtain information that a person has not willingly divulged, the principle of privacy and security in one's person and online information is disregarded. In this sense, there is a "loss of dignity, autonomy, . . . [and] respect for the individual that results when we lose control over personal information."[85] During her keynote address at the 23rd Annual Computers, Freedom, & Privacy Conference, Julie Brill, Commissioner of the FTC asked:

> [W]hat damage is done to our individual sense of privacy and autonomy in a society in which information about some of the most sensitive aspects of our lives is available for analysts to examine without our knowledge or consent, and for anyone to buy if they are willing to pay the going price[?][86]

---

[83] Sprague & Ciocchetti, *supra* note 82, at 95 (quoting Corey A. Ciochetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 56 (2007)).

[84] Jim Puzzanghera, *Tough Cookies for Web Surfers Seeking Privacy*, L.A. TIMES (Apr. 19, 2008), http://articles.latimes.com/2008/apr/19/business/fi-privacy19 [http://perma.cc/K3LE-L9WV].

[85] Nehf, *supra* note 82, at 70.

[86] Julie Brill, Commissioner, Fed. Trade Comm'n, Keynote Address at the 23rd Computers Freedom and Privacy Conference: Reclaim Your Name (June 26, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf [http://perma.cc/87MK-NF4V] (noting concerns about the fact that much of the health information that data brokers collect falls outside the stringent protections of the Health Insurance Portability and Accountability Act (HIPAA)).

The framing of this question makes it apparent that even the FTC Commissioner is uncomfortable with the way the data-collection industry treats consumer privacy.

C. Pervasiveness

There is also a concern that data brokers might be taking advantage of the widespread and pervasive nature of the Internet, which has come to be a staple of modern life. The number of Internet users in the United States increases by approximately one user per second.[87] Currently, there are over 302,050,870 Internet users in the United States,[88] a country with a population of about 321.6 million.[89] This means that about 94% of people in the United States use the Internet. Some argue that to participate fully and take advantage of modern, innovative society, one *must* have Internet access. Indeed, some courts have already recognized the indispensable nature of computer and Internet access in our modern world.[90] President Barack Obama has gone so far as to implore regulatory agencies to recognize that for most Americans, "the Internet has become an essential part of everyday communication and everyday life,"[91] emphasizing that "[t]oday[,] high-speed . . . [Internet] is not a luxury, it's a necessity."[92]

Furthermore, to accommodate commercial transactions both online and offline, businesses must ask individuals to submit some amount of personally identifiable information.[93] Simply by "participating in the Internet economy, consumers lose control over which details about their private lives are known, and they have little control over who gets to learn of these details after the data passes into a profiler's hands."[94] Are data-collection agencies taking advantage of the fact that people have little to no choice

---

[87] *See United States Internet Users*, *supra* note 10.

[88] *Id.*

[89] *U.S. and World Population Clock*, U.S. CENSUS BUREAU, http://www.census.gov/popclock/ [http://perma.cc/7VAM-232B] (last visited Dec. 11, 2015).

[90] Pollard v. Superior Cmty. Credit Union, 306 B.R. 637, 645 n.5 (Bankr. D. Minn. 2004); Schnuerle v. Insight Commc'ns, Co., L.P., 376 S.W.3d 561, 580 (Ky. 2012) (Schroder, J., concurring in part and dissenting in part) (noting that "[i]n the digital age in which we now live, internet access is becoming more and more of a necessity for personal communication, as well as for business and commerce purposes").

[91] Dashiell Bennett, *Obama: The Internet Is a Utility*, ATLANTIC (Nov. 10, 2014, 10:32 AM), http://www.theatlantic.com/technology/archive/2014/11/obama-internet-utility-fcc-regulation-net-neutrality/382561/ [http://perma.cc/W7NF-925G].

[92] Jim Kuhnhenn, *Obama Says High-Speed Broadband Is a Necessity, Not a Luxury*, DENVER POST (Jan. 15, 2015), http://www.denverpost.com/politics/ci_27322556/obama-says-high-speed-broadband-is-necessity-not [http://perma.cc/F3TW-NHBA].

[93] Sprague & Ciocchetti, *supra* note 82, at 93.

[94] Berger, *supra* note 69, at 19 (internal citation omitted).

but to reveal their information on the Internet? Is it reasonable to allow the collection of this information simply because it is there anyway? While some companies offer opt-out options for data collection, many "make opting out as cumbersome as possible" and fail to fully inform users about how their data is being used.[95] "As a result, very few people opt-out, and those who try find the process difficult and time-consuming."[96]

In the case of *In re Doubleclick Inc. Privacy Litigation*, a district court in the Southern District of New York skirted the issue of the necessary and unavoidable submission of information when it held that online advertising company Doubleclick was authorized to access plaintiff-users' "GET, POST, and GIF submissions to Doubleclick-affiliated Web sites" because these submissions were voluntary and purposeful.[97] As an online advertising company, "Doubleclick creates value for its customers in large part by building detailed profiles of Internet users and using them to target clients' advertisements."[98] In order to show the targeted advertisements to the user, Doubleclick uses cookies to collect information about a users' web activity. These cookies collect "information in three ways: (1) 'GET' submissions, (2) 'POST' submissions, and (3) 'GIF' submissions."[99] While GET and POST submissions consist of voluntarily provided information, such as terms in a search query or information provided when signing up for an online newsletter, GIF submissions track the movement of a user's mouse on a particular website.[100] Although mouse movements are certainly voluntary, one wonders how else a person could possibly browse a website without moving the mouse. Even if it were possible, GIF submissions track the cursor's movement all the same. Just because I voluntarily move my mouse does not mean I have authorized anyone to track that movement. Here lies the tension between society's inescapable need for the Internet and the individual's desire to maintain online privacy.

---

[95] Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 369 (2006).

[96] *Id.*

[97] *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001).

[98] *Id.* at 502 (internal citation omitted).

[99] *Id.* at 504.

[100] *Id.*

IV. THE CURRENT STATE OF THE LAW AND ITS KEY PLAYERS

It is important to recognize that whatever qualms exist with the data-collection industry, it is certainly here to stay. There are discernible benefits to all parties involved, and the positive impact on the economy is prevalent.[101] Extinguishing data brokers would cut off the head of a profitable and strengthening force—but this is not to say that the industry is entitled to operate with unfettered discretion. As with all things worth protecting, there must be a balance between the various interests at stake. To date, there are very few laws in place to regulate data brokers, the way data is collected, or how data is used.[102] This Part recognizes the key players involved in proposing regulations for the industry and supports several proposals that achieve a favorable balance among all interested parties.

A. The Federal Trade Commission

The regulation of data brokers is almost nonexistent.[103] The privacy laws under which data brokers currently operate have an extremely limited scope, and consumers' rights are largely unprotected, as there are "[n]o overarching federal privacy law[s] govern[ing] the collection and sale of personal information among private-sector companies."[104] Furthermore, consumers have no control over what information data brokers collect and no ability to correct inaccuracies in the collected data.[105] The FTC has led the effort to regulate the data-collection industry. The FTC's basic mission is twofold.[106] First, it seeks to "protect[ ] consumers by stopping unfair, deceptive or fraudulent practices in the marketplace."[107] To this end, the FTC "conduct[s] investigations, . . . [initiates lawsuits against] people [and companies] that violate the law, [and] develop[s] rules to ensure a vibrant marketplace."[108] Second, the FTC promotes fair

---

101 *See* DEIGHTON & JOHNSON, *supra* note 36, at 18, 23-25.

102 SENATE COMMERCE COMMITTEE, *supra* note 5, at 26.

103 *Id.*

104 U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE intro. (Sept. 2013), http://www.gao.gov/assets/660/658151.pdf [http://perma.cc/992Y-6L8L] [hereinafter GAO REPORT].

105 SENATE COMMERCE COMMITTEE, *supra* note 5, at 3.

106 *What We Do*, FED. TRADE. COMM'N, http://www.ftc.gov/about-ftc/what-we-do [http://perma.cc/HAQ6-DMUX] (last visited Dec. 11, 2015).

107 *Id.*

108 *Id.*

competition by enforcing antitrust laws and ensuring that the markets remain truly free and open.[109]

Section 5 of the Federal Trade Commission Act gives the FTC rulemaking authority with regard to various areas of consumer protection, including privacy, and allows the Commission to impose sanctions and seek monetary redress on behalf of consumers.[110] Many of the FTC's rulings and orders are considered legally binding, and Congress has authorized the majority of the regulations the FTC has published in the last two to three decades.[111]

In December 2012, the FTC conducted a study to gain insight into data broker practices.[112] In furtherance of its mission, the FTC issued Orders to File Special Reports under the FTC Act[113] to nine data brokers,[114] seeking answers to basic questions about the way each company collects, uses, and sells data.[115] In this and subsequent investigations, the FTC consistently called for increased transparency and regulation of the data-collection industry.[116] This call for transparency comes in the wake of the obvious surge in technological and societal progress and the concern that this progress will compromise individual privacy unless the law finds a way to catch up.[117]

In 2014, the FTC published another report calling for data broker transparency.[118] In this report, the Commission called on data brokers to adopt several "best practices to improve the transparency of the data broker industry."[119] First, the FTC suggested

> privacy-by-design, which includes considering privacy issues at every stage of product development. Second . . . [it] encourages data brokers to

---

[109] *Id.*

[110] *See* 15 U.S.C. §§ 41-58 (2012).

[111] JOHN A. SPAGNOLE ET AL., CONSUMER LAW CASES AND MATERIALS 6 (West Publishing Co., 4th ed. 2013).

[112] DATA BROKERS, *supra* note 21, at 7.

[113] See 15 U.S.C. § 46 (b) (2012) for the relevant portion of the Federal Trade Commission Act allowing the Commission to require certain business entities to respond to specific inquiries regarding "organization, business, conduct, practices, management, and relation [to other business entities]."

[114] DATA BROKERS, *supra* note 21, at 7-9.

[115] SENATE COMMERCE COMMITTEE, *supra* note 5, at ii. "The Committee's inquiry sought answers to four basic questions: What data about consumers does the data broker industry collect? How specific is this data? How does the data broker industry obtain consumer data? Who buys this data and how is it used?" *Id.*

[116] *See* DATA BROKERS, *supra* note 21, at 4-5, 33; s*ee also* AN ERA OF RAPID CHANGE, *supra* note 69, at 60-72 (discussing the FTC's proposal to increase data broker transparency through privacy notices, access, and consumer education).

[117] DATA BROKERS, *supra* note 21, at 5.

[118] *See id.*

[119] *Id.* at 6.

> implement better measures to refrain from collecting information from children and teens, particularly in marketing products. Finally, the Commission recommends that data brokers take reasonable precautions to ensure that downstream users of their data do not use it for eligibility determinations or for unlawful discriminatory purposes.[120]

It is the FTC's hope that these measures will help ease the tension between data brokers and consumers and create a more stable legal environment where there is a clearer delineation of what is acceptable and unacceptable.[121]

B. The Government Accountability Office

The Government Accountability Office (GAO) is also actively involved in the discussion about how to regulate the data-brokerage industry. In 2013, the FTC asked the GAO to "review the privacy laws applicable to consumer information collected and sold for marketing purposes."[122] Upon review, the GAO found that "[w]ith regard to data used for marketing, no federal statute provides consumers the right to learn what information is held about them and who holds it."[123] It also found that "consumers . . . do not have the legal right to control the collection or sharing with third parties of sensitive personal information (such as their shopping habits and health interests) for marketing purposes,"[124] and "no comprehensive federal privacy law governs the collection, use, and sale of personal information by private-sector companies."[125]

According to the GAO, few federal laws are sufficiently related in some way to consumer privacy,[126] and even fewer state laws touch on consumer privacy.[127] Of the relevant federal laws, the GAO did not find any that were specifically on point with current data-collection methods, sources, and types. It found that "the scope of current federal privacy laws is limited in addressing the methods by which, or the sources from which,

---

120 *Id.* at ix.

121 *Id.* at vii.

122 SENATE COMMERCE COMMITTEE, *supra* note 5, at 3.

123 GAO REPORT, *supra* note 104, at intro.

124 *Id.*

125 *Id.* at 7.

126 *Id.* The GAO makes special mention of the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, HIPAA, the Children's Online Privacy Protection Act, the Electronic Communications Privacy Act, the Federal Trade Commission Act, the Telecommunications Act, and the Computer Fraud and Abuse Act. *Id.* at 8-14. Although all of these federal acts address consumer privacy protection in one way or another, they are narrowly tailored and apply to very specific circumstances. *Id.* at 7.

127 *Id.* at 14.

information resellers and private-sector companies collect and aggregate personal information, or the types of information that may be collected for marketing or look-up purposes."[128] Furthermore, "[t]he current privacy framework does not fully address new technologies[,] . . . such as social media, web tracking technologies, and mobile devices[, that] have enabled even cheaper, faster, and more detailed data collection and sharing among resellers and private-sector companies."[129]

As for state laws, the GAO found that California, Utah, Massachusetts, and Nevada all have laws that address the issues with which the FTC and GAO are concerned. "California's Shine the Light law requires certain businesses to disclose, upon a California customer's request, whether those businesses have shared the customer's personal information with third parties for direct marketing purposes."[130] Utah has a similar law requiring "commercial entities to disclose to consumers the types of nonpublic personal information shared with or sold to third parties for compensation."[131] Both Massachusetts and Nevada "have laws or regulations requiring businesses to safeguard and encrypt personally identifiable consumer data."[132] In assessing the minimal findings in both federal and state law, the GAO determined that there are indeed gaps in both federal and state privacy law schemes and suggested a baseline framework that would help fill in those gaps on a federal level, allowing states to fill in the rest.[133] At a minimum, what the federal government should guarantee to consumers is a level of privacy on par with the values and social norms reflective of a twenty-first-century society.

C. Proposed Legislation

In March 2015, four U.S. Senators introduced the Data Broker Accountability and Transparency Act (DATA Act),[134] which calls upon the FTC to promulgate concrete rules for data

---

[128] *Id.* at 18.

[129] *Id.* at 19.

[130] *Id.* at 15; *see* CAL. CIV. CODE § 1798.83 (effective Jan. 1, 2005).

[131] GAO REPORT, *supra* note 104, at 15; *see* UTAH CODE ANN. §§ 13-37-101 to -203 (West 2003).

[132] GAO REPORT, *supra* note 104, at 15; *see* 201 MASS. CODE REGS. 17.01 to 17.05 (2010); NEV. REV. STAT. §§ 603A.010 to .920 (2011).

[133] GAO REPORT, *supra* note 104, at 31-33.

[134] Data Broker Accountability and Transparency Act of 2015, S. 668, 114th Cong. (2015) (introduced in the Senate on March 4, 2015); John M. Simpson, *Consumer Watchdog Backs Senate Data Broker Accountability and Transparency Act*, CONSUMER WATCHDOG (Mar. 5, 2015), http://www.consumerwatchdog.org/newsrelease/consumer-watchdog-backs-senate-data-broker-accountability-and-transparency-act [http://perma.cc/T9G5-CPCP].

collection. The DATA Act would require all data brokers to "maintain an Internet website and place a clear and conspicuous notice on the Internet website"[135] with instructions for how individuals can review personal information previously collected or assembled by the data broker and how to express a preference with respect to the use of personal information for marketing purposes.[136] Under the Act, individuals would have an automatic right to access information that data brokers collect about them.[137] Upon request, data brokers must grant an individual access to any personal information that the data broker has collected about him or her and allow the individual to correct any information that may be inaccurate.[138] Perhaps the most satisfying requirement for those who find tailored online advertisements unfavorable, the DATA Act obligates any data broker that collects personal information and "uses, shares, or sells that information for marketing purposes" to provide data subjects "with a reasonable means of expressing a preference not to have . . . [their] information used for those purposes."[139] This opt-out mechanism is extremely important for building a relationship of trust between data brokers and consumers. This section of the Act, however, provides an opt-out mechanism only for the specific activities and purposes mentioned. The language of the Act implicitly gives data brokers permission to collect information for other purposes, and it provides no further opportunity to opt out.[140]

Giving individuals choices about what information about them (if any) is collected would alleviate at least some concerns about the lack of transparency in the data-collection industry. The DATA Act has been referred to the Committee on Commerce, Science, and Transportation and awaits further review. But despite the widespread public interest group support for the bill,[141] govtrack.us has determined that there is only a four percent chance of its enactment.[142] This strikingly low number is unfortunate given the implications if the bill is

---

[135] Data Broker Accountability and Transparency Act of 2015, S. 668, 114th Cong. § 4(d)(1) (2015).

[136] *Id.*

[137] *Id.* § 4(b)(1).

[138] *Id.* § 4(f)(1).

[139] *Id.* § 4(e). It is worth noting that many companies not considered data brokers allow users to access and correct any personal information that the company may have pursuant to an online privacy policy or similar engagement form.

[140] *Id.* § (e)(f)(2).

[141] Simpson, *supra* note 134.

[142] *S. 688: Data Broker Accountability and Transparency Act of 2015*, GOVTRACK.US, https://www.govtrack.us/congress/bills/114/s668 [http://perma.cc/GD8S-Y5M2] (last visited Dec. 11, 2015).

passed.[143] Its provisions would change the face of the data-brokerage industry and help alleviate many concerns expressed by government agencies and consumers alike.

The need for regulation of the data-collection industry cannot be stressed enough. Regulation that comports with the FTC's aims would create the transparency and accountability that the various state and federal agencies seek to achieve. Any regulations or legislation must account for all of the interests at stake. Successful propositions will strike a balance between consumer and industry needs; to this end, measures must be reasonable. These measures must keep pace with the rapid and constant technological change in this country in order to ensure that technology and the law do not collide, stifling one another's progress.

V. SHOW ME THE MONEY: A PROPOSAL TO EASE THE TENSION BETWEEN DATA BROKERS AND CONSUMERS

There is little doubt that the recent proposals for targeted regulation of the data-collection industry are giant leaps forward in the otherwise wild west-type landscape that currently exists. These promising steps signal a positive move toward easing the tensions between data brokers, consumers, and other interested parties. Notwithstanding this progress, these bills remain stagnant in Congress and have a depressingly low chance of enactment.[144] Luckily, there may be another way to ease this tension: compensate consumers for their data.

If the strain between data brokers and consumers is to be truly alleviated, it is imperative that consumers—the individuals who by their own virtual and physical presence create the mountains of information that are worth billions of dollars a year to data brokers—feel like they are being treated fairly. Relationships are about compromise, and it seems that data brokers are doing far more taking than giving. Instead of being rewarded and compensated for their obviously valuable assistance, consumers feel uninformed and deceived by data brokers' conduct. Every single mouse click, URL entry, and Google search goes into creating consumers' valuable profiles. It is the consumer's existence that fuels the data-collection industry—

---

[143] According to govtrack.us, "only 15% of bills made it past committee and only about 3% were enacted in 2013–2015"—statistics that do not bode well even for bills with chances of enactment many times higher than that of the DATA Act. *Id.*

[144] *See supra* Section IV.C.

without them, data brokers have nothing to collect and nothing to sell. A system of compensation, whether monetary or otherwise, would strengthen this relationship and allow for balance between data brokers' business interests and consumers' and society's interests in integrity, privacy, and self-worth.

Many plaintiffs have turned to courts with a similar thought in mind.[145] A common claim brought in this context is that of unjust enrichment. Although elements of an unjust enrichment claim may vary from state to state,[146] "[t]he pivotal concept of unjust enrichment is the occurrence of a wrong or something unjust. The mere fact that a defendant may have benefitted from the plaintiff's action alone is insufficient to grant relief . . . ; it must be shown that the defendant's enrichment is unjust."[147] An unjust enrichment claim is a common theory of liability in contract law and is thought of as a quasi-contract claim.[148] Courts have largely ignored unjust enrichment claims in relation to data collection and claims alleging that data collectors should compensate Internet users for their personal information.

In the case of *In re Nickelodeon*,[149] a class of plaintiffs consisting of children under the age of 13 alleged that defendants Viacom and Google violated their privacy rights by placing both first- and third-party cookies on their computers without either their consent or the consent of their parents.[150] These cookies allowed defendants to collect information about the children's identities and Internet activity and compile this information with previously gathered data.[151] In their complaint, the plaintiffs contended that personal information *is* valuable.[152] They stated that "[t]he value of the information that Defendants take from people who use the Internet is well known . . . . Personal information is now viewed as a form of currency."[153] The district court for the District of New Jersey

---

[145] *In re* Google Inc. Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434 (D. Del. 2013); *In re* Nickelodeon Consumer Privacy Litig., No. 2443 (SRC), 2014 U.S. Dist. LEXIS 91286 (D.N.J. 2014); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

[146] *See* 66 Am. Jur. 2d Restitution and Implied Contracts § 11 (outlining the different approaches that states take with respect to pleading unjust enrichment).

[147] 42 CORPUS JURIS SECUNDUM IMPLIED CONTRACTS § 9 (footnote omitted); N.Y. PRAC., CONTRACT LAW § 4:12.

[148] *In re* Nickelodeon, 2014 U.S. Dist. LEXIS 91286, at *18-20.

[149] *Id.*

[150] *Id.* at *6-10.

[151] *Id.*

[152] *Id.* at *14.

[153] *Id.*

declined to agree with this proposition, noting that even if the plaintiffs' claim about the value of personal information was true, "it does not follow that personal information of the type collected by Viacom and Google has actual monetary value to Plaintiffs themselves."[154] In proffering this analysis, the court overlooked the crucial fact that without individuals like the class of plaintiffs at bar, Google, Viacom, and similar companies would have no data to collect at all.

In rejecting the plaintiffs' contentions, the court drew an interesting comparison, stating that the plaintiffs' claim was "indistinguishable from the belief that a football fan could sell her eyeballs to a TV network for four cents because an advertiser pays $4 million to reach 100 million viewers during the Super Bowl."[155] With all due respect to the court and its opinion, these acts are simply not comparable. Once one's eyeballs are sold, the consumer, who can no longer use his ocular sense, is a useless consumer to the TV network. On the contrary, an Internet user is a perpetual source of income for data brokers. A single individual's data set can be sold a limitless number of times to as many people as are willing to pay for it. The only thing that would stop a user from creating collectable data in such a permanent way as removing one's eyeballs would be to ensure that said user never accessed a computer and never left his or her house. It is essential that courts recognize this symbiosis and acknowledge it as unique from a typical consumer-business relationship.

The *Nickelodeon* "[p]laintiffs argue[d] that . . . [Google and Viacom] 'received a direct benefit' from the information they collected from [the plaintiffs]."[156] This would appear to be a rather accurate statement of what occurred. The defendant companies undoubtedly benefitted from the plaintiffs' information. The court, however, interpreted unjust enrichment to "require[] that the plaintiff show that it expected remuneration from the defendant at the time it performed or conferred a benefit on defendant and that the failure of remuneration enriched defendant beyond its contractual rights."[157] When analyzing the plaintiffs' claim, the court stated that a

> receipt of a benefit by a defendant and conferral of a benefit by a plaintiff are two different things, and it simply is not reasonable for

---

[154] *Id.* at *15.
[155] *Id.* at *14-15.
[156] *Id.* at *70.
[157] *Id.* at *69 (quoting VRG Corp. v. GKN Realty Corp., 641 A.2d. 519 (N.J. 1994)).

> a consumer—regardless of age—to use the Internet without charge and expect compensation because a provider of online services has monetized that usage.[158]

Looking at the Internet in this way is a dangerous game. To say that data brokers can do whatever they want with online information simply because the Internet is a "free" service (which may not necessarily be the case) and the user already benefits by using the service in the first place would open the door to a flood of adverse online activity from which users should be protected—even if the service is free.

Despite the various studies on the value of data and the clear market value of the data-collection industry,[159] courts have been unwilling to recognize that personal information has an enhanced monetary value when in the hands of a data broker.[160] *In re Google* addressed the defendants' usage and placement of first- and third-party cookies on its site and affiliated sites. The plaintiffs brought suit because they were unhappy about the targeted ads showing up on their Internet browsers and believed that defendant companies tricked their "browsers into accepting cookies, which then allowed defendants to display targeted advertising."[161] The court found that the plaintiffs did not plead facts sufficient to show that they had sustained an injury in fact as a result of the defendants' data collection.[162] Although the plaintiffs "offered some evidence that the online personal information at issue ha[d] some modicum of identifiable value to an individual plaintiff," they "[did] not sufficiently allege[] that the ability to monetize their PII ha[d] been diminished or lost by virtue of Google's previous collection of it."[163] Similarly, in *LaCourt v. Specific Media, Inc.*, the fact that a third party collected the plaintiffs' personal information was not enough to establish that the plaintiffs were deprived of some economic value.[164]

It makes little sense that when a third party collects a person's data and sells it for a profit, the act is not sufficient to show that that the third party has deprived the individual of that data's value. It also seems somewhat intuitive that a person should be paid for the use of his or her creation,

---

[158] *Id.* at *70.

[159] *See supra* Section I.C; DEIGHTON & JOHNSON, *supra* note 36.

[160] *See In re* Google Cookie Placement Privacy Litig., 988 F. Supp. 2d. 434 (D. Del. 2013).

[161] *Id.* at 439.

[162] *Id.* at 442.

[163] *Id.* (internal citation omitted).

[164] LaCourt v. Specific Media, Inc., No. 10-1256-GW (JCGx), 2011 U.S. Dist. LEXIS 50543, at *12 (2011).

especially when that person has already done the hard part of making something out of nothing. There should be a way to compensate this creator. Like a shareholder's dividend, data brokers could pay consumers at year's end for the relative value of their information. Although this amount may end up being very little,[165] it is much more about the principle—individuals playing an active role in how others use their information as opposed to being passively taken advantage of—than being paid a handsome profit. Alternatively, data brokers could offer special benefits, such as coupons or vouchers for products or services in which that consumer has an interest. The consumer would benefit from the data broker's tailored product suggestions, and the data broker would continue to profit from selling the consumer's information. In fact, an interesting experiment conducted at a Brooklyn arts festival determined that consumers were significantly more likely to give up personal information if they had an incentive.[166] Like the saying goes, you catch more flies with honey.[167]

It is also unclear why the law provides protections in copyright and intellectual property for original works and expressions but declines to protect unique lists of information that are just as personal and identifiable as a musical composition or the manifestation of an idea on paper. This is not to say that an entirely new legal right or cause of action need be created; however, it is important to recognize, at the very least, that individuals think about their personal

---

[165] Emily Steele et al., *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013, 8:11 PM), http://www.ft.com/cms/s/2/927ca86e-d29b-11e2-88ed-00144feab7de.html [http://perma.cc/5XEN-5DFU] (noting that "[t]he average person's data often retails for less than a dollar").

[166] Lois Beckett, *How Much of Your Data Would You Trade for a Free Cookie?*, PROPUBLICA (Oct. 1, 2014, 12:00 PM), http://www.propublica.org/article/how-much-of-your-data-would-you-trade-for-a-free-cookie [http://perma.cc/4RZP-PZFV]. In this piece of performance art turned social experiment, entitled "Please Enable Cookies," artist Risa Puno offered 380 New Yorkers fresh baked cookies in exchange for their personal information. Puno asked for things like name, address, phone number, and driver's license number. Out of those 380 people, almost half were willing to give more sensitive information, such as the last four digits of their Social Security number. One-third were willing to have their fingerprints taken.

[167] Omar Tene and Jules Polonetsky, two prominent figures in the field of online privacy, have suggested a similar framework for recognizing the value of an individual's information whereby companies share with individuals the information they have about them in a "'useable format'" that would "allow[] them to take advantage of third party applications to analyze their own data and draw useful conclusions." Omar Tene & Jules Polonetsky, *Big Data For All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH & INTELL. PROP. 239, 264 (2013). This framework would allow users to create value from their information as opposed to receiving a monetary payout from the company itself. *Id.*

information as something in which they have an interest. According to one commentator,

> It is likely too late to suggest that consumers actually do *own* their information, and that we should, therefore, analyze the rights of profilers based on a concept of a license to use the data. Nonetheless, the best solutions in this area must accommodate the concept that consumers think of personal information as their property, and their privacy and ownership expectations reflect this.[168]

At present, a startup called Datacoup provides a service in which registered users can receive cash in exchange for access "to a combination of their social media accounts, such as Facebook and Twitter, and the feed of transactions from a credit or debit card."[169] The company "believe[s] that everyone has valuable data" and allows people to capitalize on that data.[170] This type of initiative presents an example of a compensation structure in real time, and its implementation is significant. By offering to pay participants for their data, it solidifies the notion that one's personal information is indeed valuable. The compensation scheme then gives back to the consumer for providing the information, which the company has already recognized as valuable. Furthermore, Datacoup exemplifies how private citizens and companies can come together to solve problems independently of legislatures and outside of the courtroom.

CONCLUSION

As technology continues to develop, society must face new and different social and legal issues. The existence of data brokers and data-collection companies raise these issues. The privacy concerns surrounding data collection will not disappear, and unless specific measures are taken, the data-brokerage industry will continue to operate unregulated. It is imperative to address these concerns to prevent them from spinning out of control and setting a laissez-faire precedent.

While no problem can be solved overnight, one step toward filling the regulatory gap is for data brokers to publicly acknowledge the fact that consumers and Internet users are

---

168 Berger, *supra* note 66, at 60 (internal citation omitted).

169 Tom Simonite, *Sell Your Personal Data for $8 a Month*, MIT TECH. REV. (Feb. 12, 2014), http://www.technologyreview.com/news/524621/sell-your-personal-data-for-8-a-month/ [http://perma.cc/L9QL-TKZL]; *How It Works*, DATACOUP, https://datacoup.com/docs#how-it-works [http://perma.cc/5CQ9-9SAA] (last visited Dec. 11, 2015).

170 DATACOUP, *supra* note 169.

not only an integral part of their business, but a necessary part, as well. The value of collected information cannot be overstated. Data collection's tremendously positive impact on the U.S. economy, as well as the fact that data brokers sell collected information for a substantial profit, demonstrates how lucrative consumer information really is. Compensating consumers for their information would certainly signal data brokers' acknowledgement not only of the monetary value of personal information, but also of the intrinsic value of a dossier of information that conjures up a near complete image of an individual's life.

Legislatures and courts must take proactive steps to address the various concerns surrounding the data-collection industry and develop real solutions recognizing that all interested parties have different yet equally important rights worth protecting. Even if the law drives in a slower lane than technology, initiatives like Datacoup prove that compromises do not always have to involve attorneys and judges.

Let us think back to our trip to the grocery store, back to the key lime pie, the diapers in the shopping cart, and the personal-space-invading tailgater. Now that we have all the items we need for our pie, it is finally time to head to the checkout lane and be rid of the pesky follower. All the items are on the conveyor belt, and the clerk asks to scan your rewards card. Then, when you get home, you pull up the recipe from the Food Network website on your iPad. The single grocery store tailgater morphed into at least two virtual tailgaters with just a swipe and a click. Even though data brokers commit no physical intrusion, an intangible and metaphysical intrusion occurs. The line between physical and virtual space is not just blurred—it is almost gone completely. It is society's responsibility to determine the destiny of this line. Will we preserve it, or will we let it fade into the technosphere?

Julia N. Mehlman[†]

---

† J.D. Candidate, Brooklyn Law School, 2016; B.A., University of Delaware, 2013. Thank you to the staff of the *Brooklyn Law Review* for all of their hard work. A special thanks to Lillian Smith, Steven Ballew, and Michael Piacentini for all of their help and incredible attention to detail above and below the line. Thank you to all of my friends and family for their continued love and support, with a special mention given to my brother Tyler Mehlman for always keeping me on my toes. Thank you to Matthew Klepacki for his patience and encouragement throughout the writing process. Last, and most importantly, I would like to thank my parents, Scott Mehlman and Laura Mehlman, for nurturing my love of reading and learning throughout my life and for always loving and supporting me in everything I do.